

**IT ACCEPTABLE USE**

Department	Administration	Policy No.	0340-001
Section	Information Technology	Date Approved by Board	November 28, 2019
Repeals		Board Resolution #	RD/19/11/21 (28)

Amended		Board Resolution #	
Amended		Board Resolution #	
Amended		Board Resolution #	

Repealed		Board Resolution #	
----------	--	--------------------	--

1. Purpose

- 1.1 The purpose of the IT Acceptable Use Policy is to define the acceptable uses of Information Technology (IT) Resources that support the Peace River Regional District (PRRD). The PRRD provides access to IT Resources for work purposes that serve the interests of the Regional District.

2. Scope

- 2.1 This Statement of Policy applies to the PRRD Regional Board, staff, hired contractors, and other individuals with access to PRRD IT Resources and/or IT Devices.

3. Definitions

- 3.1 *Acceptable Personal Use*: defined as reasonable and limited personal communication, including occasional use of apps and web browsing.
- 3.2 *Authorized User*: Any person who is granted access to IT Resources or IT Devices. Authorized Users can include employees, elected officials, contractors and other individuals.
- 3.3 *Cloud-Based Service*: A term that refers to applications, services, or resources made available to users on demand via the internet from a cloud computing provider's servers.
- 3.4 *E-discovery*: refers to the preservation, retrieval, exchange, and production of documents from electronic sources in electronic form.
- 3.5 *Freedom of Information and Protection of Privacy Act (FOIPPA)*: refers to the Act that sets out the access and privacy rights of individuals as they relate to the public sector.
- 3.6 *IT Resource*: An application server, network share, wireless or wired network, domain controller, printer, cloud-based service, or other similar resource.
- i. *PRRD Network*: Any physical or virtual network at the PRRD, including wireless and wired connections.
- 3.7 *IT Device*: Any end-user device which can be a laptop, desktop, smartphone, tablet computer, or other similar device.
- i. *Corporate Issued Devices*: Any IT Device issued and managed by the PRRD provided to an individual.



- 3.8 *Least Privilege Needed*: refers to a principle requiring that each subject in a system be granted the most restrictive set of privileges (lowest clearance) needed to perform their employment duties. The application of this principle limits the damage that can result from accident, error or unauthorized use.
- 3.9 *Need to Know*: refers to a principle where access is restricted to authorized Employees that require it to carry out their work. Employees are not entitled to access merely because of status, rank, or office.
- 3.10 *Portable Data Storage Device*: USB sticks, portable hard disks, CD/DVDs, and other similar devices.
- 3.11 *Public Body*: refers to the ministries of the B.C. and Canadian federal governments; an agency, board, commission, corporation, office; a local public body; or any other body that may be covered by [FOIPPA](#).
- 3.12 *Service Set Identifier (SSID)*: used to broadcast WiFi networks.
- 3.13 *Software-as-a-Service*: a software distribution model in which a third-party provider hosts applications and makes them available to customers over the internet.
- 3.14 *Telephony Service*: the field of technology involving the development, application, and deployment of telecommunication services for the purpose of electronic transmission of voice, fax, or data, between distant parties.
- 3.15 *Two-Factor Authentication*: an extra layer of security that requires not only a password and username but also something available, such as a token or a code texted to the user for verification.

4. Policy

4.1 Monitoring of Activity

- a. Use of [IT Resources](#) creates activity records, including but not limited to, network logons, server file activity, email traffic, and internet traffic.
- b. Any collection, access, use, transmission, or disposal of data or use of PRRD IT Resources, whether for personal reasons or not, may be audited, inspected, monitored and/or investigated to:
 - i. maintain, repair, and manage [IT Resources](#) for the efficient operation of systems;
 - ii. meet legal requirements to produce information, including by engaging in [e-discovery](#);
 - iii. ensure accessibility of IT Resources for the continuity of work processes;
 - iv. improve business processes and manage productivity; and,
 - v. ensure compliance with policy and legislative requirements.
- c. The Regional District reserves the right to review the use of its [IT Resources](#). [Authorized Users](#) should be aware that they have no right to ownership or expectation of privacy with respect to their use of the IT Resources and the use will be monitored.
- d. Email and data stored on the [PRRD Network](#) are regularly backed up and stored, and are recoverable, even if the original files, documents, email, or data have been deleted by the user.



4.2 Accounts and Authentication Security

- a. [Authorized Users](#) must not divulge, share, or compromise their own or another's authentication credentials (e.g. passwords, access cards, etc.). This includes not divulging passwords to technical support over email, phone, or other electronic means.
- b. Authorized Users may be held accountable for all activities that occur under their authentication credentials and should immediately report any known or suspected compromise to the IT Department.
- c. Generic accounts such as "anonymous" or "guest" are not permitted.
- d. The password length, complexity, and formation is determined by the IT Manager.
- e. Authorized Users must inform the IT Manager of the use of any externally accessible [IT Resources](#) for conducting PRRD business.
- f. When accessing [cloud-based services](#), Authorized Users must use strong passwords or utilize a second layer of protection such as a [two-factor authentication](#), when possible.

4.3 IT Device Security

- a. Access to PRRD [IT Devices](#) is restricted to [Authorized Users](#) only.
- b. Authorized Users must not modify, alter, or remove physical or software components that could affect the integrity or security of the IT Device or the [PRRD Network](#). Any security protection must not be disabled.
- c. Authorized Users who leave their equipment/devices unattended must log off or lock the device to prevent unauthorized access to the device. Mobile devices, such as smartphones and tablets, must include a passcode and auto-lock after five (5) minutes or less.
- d. When using portable IT Devices (such as laptops, smartphones, tablets, other similar devices) the Authorized Users must:
 - i. store PRRD data and files on the PRRD Network servers and are strongly discouraged from storing PRRD data on their local hard disks or removable media;
 - ii. only store data on [portable data storage devices](#) in extenuating circumstances, and the data must be encrypted;
 - iii. not attach any non PRRD-issued devices to the Corporate Network without express consent from the IT Department.
- e. Authorized Users are responsible to return all PRRD IT Devices, PRRD data, and intellectual property to the IT Department upon termination or departure.
- f. Any lost or stolen PRRD IT Devices or PRRD data must be reported to the Corporate Officer and the IT Department immediately.



4.4 Email, Internet, and Network Usage

- a. All business being conducted for the PRRD must be done through PRRD-assigned emails, even when work is conducted outside of the workplace.
 - i. Only in extenuating circumstances may personal accounts be used to conduct PRRD business, and all emails must be copied to the PRRD mail server.
- b. PRRD emails are not to be automatically forwarded to outside email addresses, unless such outside email address has been issued by a [public body](#) subject to [FOIPPA](#).
- c. The PRRD reserves the right to filter and quarantine both inbound and outbound electronic content, including but not limited to email and web content.
- d. [Authorized Users](#) must never send credit card information, account passwords, financial information, politically sensitive information, or extensive personal information in an email unless the user confirms that the recipient is who they claim to be via alternative methods.
- e. Precautions must be taken when opening or acting on an email. The sender of an email must be verified before acting on the content in an email, especially emails dealing with financial transactions or authorizations.
- f. When using PRRD [IT Resources](#), Authorized Users must not:
 - i. download, display, or distribute any explicit, discriminating, threatening, harassing, or offensive graphic or document. Explicit material may not be archived, stored, distributed, edited, or recorded using PRRD IT Resources;
 - ii. deliberately or carelessly propagate any virus or malware on the [PRRD Network](#);
 - iii. forward email spam or malware, unless requested by the PRRD IT Department;
 - iv. access any material which contravenes the *BC Human Rights Act*, *Criminal Code*, or any Federal or Provincial Law;
 - v. access online gambling or gaming websites; and,
 - vi. disable or overload any IT Resource (computer system or network).
- g. Third party cloud synchronization services that host data outside of Canada and do not comply with [FOIPPA](#) regulations (e.g. Dropbox, Google Apps, etc.) are prohibited for storing PRRD records.
- h. All email communication must comply with *Canada's Anti-Spam Legislation*.
- i. Incidental usage of the Internet, [IT Resources](#), and [IT Devices](#) for personal use (such as personal activities and viewing personal email accounts) are permitted but limited to breaks, lunch breaks, outside core working hours, or in an emergency situation, and must:
 - i. not detract from work responsibilities or job performance;
 - ii. not impair the normal functioning of an IT Resource or interfere with another's use of an IT Resource;
 - iii. not result in PRRD incurring an expense;
 - iv. not result in personal financial gain (e.g. derive income from a secondary source); and,



- v. remain in compliance with this policy.

4.5 Software Application Usage

- a. [Authorized Users](#) must never store, install, or use software that is not purchased by or licensed by/or licensed to the PRRD. Any such files or software may be used only in ways that are consistent with their licenses.
- b. Authorized Users are not to make copies of copyrighted software unless the appropriate software licensing allows it.
- c. Authorized Users must have their supervisor's permission to download or use applications or software downloaded from the internet, USB, or installed from a CD/DVD.
- d. Supervisors must not permit an Authorized Users to download or use applications or software that are prohibited by the IT Manager, present unacceptable privacy or security concerns, and/or impose unacceptable terms and conditions.

4.6 Mobile Device Usage

- a. Eligibility for corporate issued mobile devices will be limited to [Authorized Users](#) who meet one or more of the following criteria:
 - i. who spend the majority of their time working outside of the office;
 - ii. whose job duties are in public safety, requiring immediate or emergency response;
 - iii. who job duties support full-time business infrastructure and systems;
 - iv. who are required to respond promptly to urgent business related email or communication;
 - v. in other situations where a "business case" has been approved by the CAO.
- b. In response to a *Freedom of Information and Protection of Privacy* request, any information stored on the Corporate-issued mobile device is subject to that request.
- c. [Authorized Users](#) are responsible for applying operating system and mobile app updates on a regular basis on Personally-owned and Corporate-issued devices connecting to the [PRRD Network](#).
 - i. The IT Manager reserves the right to revoke access to any device connecting to the PRRD Network.
- d. Authorized Users must not change or alter the operating or security systems on a Corporate-issued or personally-owned mobile device that is accessing the PRRD Network.

4.7 Wireless Security

- a. All staff PRRD-issued [IT Devices](#) are to connect to the Corporate wireless network. PRRD Directors' IT Devices and personally owned IT Devices may connect to the PRRD Public or **PRRD Corporate** wireless network.



- b. No installations of unauthorized parallel wireless infrastructure and/or rogue wireless devices are permitted on the [PRRD Network](#) or within the PRRD facilities.
- c. If an [IT Device](#) or piece of equipment is found to be causing interference with PRRD's wireless (WiFi) network, IT will disable or remove the device.

4.8 Remote Access

- a. Remote access is not provided to all [Authorized Users](#) and is granted by the supervisor.
- b. Authorized Users must not leave any [IT Device](#) unattended when remotely logged into the [PRRD Network](#), without taking the appropriate security precautions.
- c. Authorized Users are expected to apply the same safeguards, prudence, and due diligence when working outside the workplace as they do when in the workplace.
- d. Authorized Users are responsible for making sure that antivirus is installed and updated when connecting remotely to the PRRD Network, whether the device is owned by the PRRD or not.
 - i. The IT Manager reserves the right to revoke access to any device remote accessing the PRRD Network.

4.9 Contractor Access to Network

- a. The use of the PRRD [IT Resources](#) by outside consultants or unauthorized users shall only be done with prior approval of the PRRD IT Manager.
- b. External access by a Contractor or unauthorized user to PRRD IT Resources require a signed *Contractor Device Access Agreement*.
- c. A *Data Sharing Agreement* contract is required when sharing data with another organization, person, or business, and must be signed by both parties before access is provided.

4.10 PRRD Network Infrastructure

- a. PRRD servers and network equipment must be kept in a temperature-controlled, locked room with access limited to personnel responsible for the support of the servers. The servers and network equipment must be connected to battery-backup equipment.
- b. PRRD [IT Devices](#) must utilize disk-layer data encryption, whenever possible.
- c. With the exception of mobile devices (e.g. laptops, smartphones, tablets, other similar devices), relocation of IT Devices and equipment must be approved by the IT Manager.
- d. Staff must follow proper hard disk erasure measures before any PRRD IT Devices are released for resale.
- e. PRRD monitors and manages the total storage capacity of PRRD [IT Resources](#) and can, at any time, restrict individual storage capacity to ensure business resilience and continued service levels. This includes email mailboxes, storage on the [PRRD Network](#), IT Device, or other similar IT storage resources/devices.



- f. Technology purchasing must be approved by the IT Manager to ensure that:
 - i. [IT Resources](#) are not negatively impacted;
 - ii. the technology complies with privacy legislation and policy; and,
 - iii. standards and interoperability are maintained.
- g. The IT Manager must maintain a Hardware Refresh Cycle Plan to ensure all PRRD IT Resources and [IT Devices](#) are in high working order.

4.11 User Management

- a. Access to [IT Resources](#) are based on “[Least Privilege Needed](#)” and “[Need to Know](#)” principles to balance PRRD IT Resource security and the job responsibilities of the [Authorized User](#).

Affiliated Procedure	
----------------------	--